What is claimed is:

1. A method for monitoring technology information for vulnerabilities, the method comprising an automated workflow process for:

detecting a vulnerability;

researching the vulnerability; and

documenting the vulnerability within vulnerability data.

2. The method of claim 1, wherein the automated workflow process further comprises:

reviewing the vulnerability and the vulnerability data;

editing the vulnerability data;

approving the vulnerability and the vulnerability data; and

publishing the vulnerability and the vulnerability data to a database.

3. The method of claim 1, wherein at each step in the workflow process, reference data including a reference name, reference number and a technology name can be added to the vulnerability data and the reference data will be presented to an approver for approval.

4. The method of claim 1, wherein at each step in the workflow process, workflow comments can be added to the vulnerability data and the workflow comments can be displayed during the steps of the workflow process with the most recent addition being shown first.

5. The method of claim 1, wherein technology information is added to the vulnerability data in a hierarchical structure, said technology information at least comprising:

vendor information;

product information; and

release information.

6. The method of claim 1, wherein automated workflow process steps are performed by one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task is a single vulnerability at a single process step within the automated workflow process.

7. The method of claim 6, wherein said one or more users are assigned a level of experience that can be used by the automated workflow process to determine a level of review required for said one or more users.

8. The method of claim 6, wherein said one or more users are assigned to one or more groups of users, wherein the tasks may be assigned to a group of users of said one or more groups of users any one of said one or more users may open the task, wherein a user within said group must open the task before the user can perform a process step associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the vulnerability data.

9. The method of claim 6, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user of said one or more users wherein said user can change the way the task list is displayed.

10. The method of claim 6, wherein said one or more users login to the automated workflow process using a login name and a password with said automated workflow process capturing data indicating how long said users remain logged in, where said captured data is used to generate a report.

11. A method for monitoring technology information for configuration standards comprising an automated workflow process for:

initiating a configuration standard;

researching the configuration standard; and

documenting the configuration standard within configuration standard data.

12. The method of claim 11, wherein the automated workflow process further comprises:

reviewing the configuration standard and the configuration standard data;

editing the configuration standard data;

approving the configuration standard and the configuration standard data; and

publishing the configuration standard and the configuration standard data to a database.

13. The method of claim 11, wherein at each step in the workflow process, reference data including a reference name, reference number and a technology name can be added to the configuration standard data and the reference data will be presented to an approver for approval.

14. The method of claim 11, wherein at each step in the workflow process, workflow comments can be added to the configuration standard data and the workflow comments can be displayed during the steps of the workflow process with the most recent addition being shown first.

15. The method of claim 11, wherein technology information is added to the configuration standard data in a hierarchical structure, said technology information at least comprising:

vendor information;

product information; and

release information.

16. The method of claim 11, wherein automated workflow process steps are performed by one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task within said list of tasks is a single configuration standard at a single process step within the automated workflow process.

17. The method of claim 16, wherein said one or more users are assigned a level of experience that can be used by the automated workflow process to determine a level of review required for a user.

18. The method of claim 16, wherein said one or more users are assigned to one or more groups of users, wherein the task may be assigned to a group of users any one of whom may open the task, wherein a user within said group opens the task before the user can perform a process step associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the configuration standard data.

19. The method of claim 16, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user with said one or more users wherein said user can change the way the task list is displayed.

20. The method of claim 16, wherein said one or more users login to the automated workflow process using a login name and a password with said automated workflow process capturing data indicating how long each of said users remain logged in, where said captured data is used to generate a report.

21. A method for developing configuration standards for use with an automated workflow process comprising:

initiating a content entry;

researching the content entry;

validating the content entry;

approving the content entry; and

publishing the content entry to a database of approved configuration standards.

22. A method for updating content within a content management system using an automated workflow process, wherein content within the content management system is

updated by a Content Update System that uses a pull methodology by allowing systems to obtain updated content when requested rather that pushing data onto said systems.

23. A method for creating policies for use within a content management system using an automated workflow process, comprising:

initiating a content entry;

researching the content entry;

validating the content entry;

approving the content entry; and

publishing the content entry to a database of approved policies.

24. An automated workflow system for monitoring technology information for vulnerabilities comprising:

a detector for detecting a vulnerability;

a researcher for researching the vulnerability; and

a documenter for documenting the vulnerability within vulnerability data.

25. The system of claim 24, wherein the automated workflow system further comprises:

a reviewer for reviewing the vulnerability and the vulnerability data;

an editor for editing the vulnerability data;

an approver for approving the vulnerability and the vulnerability data; and

a publisher for publishing the vulnerability and the vulnerability data to a database.

26. The system of claim 24, wherein each device of the workflow system can add reference data including a reference name, reference number and a technology name to the vulnerability data and the device presents reference data to an approver for approval.

27. The system of claim 24, wherein each device of the workflow system can add workflow comments to the vulnerability data and the workflow comments can be

displayed by the devices of the workflow system with the most recent addition being shown first.

28. The system of claim 24, further comprising technology information added to the vulnerability data in a hierarchical structure, said technology information at least comprising:

vendor information;

product information; and

release information.

29. The system of claim 24, further comprising one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task is a single vulnerability at a single device within the automated workflow system.

30. The system of claim 29, wherein said one or more users are assigned a level of experience that can be used by the automated workflow system to determine a level of review required for said one or more users.

31. The system of claim 29, wherein said one or more users are assigned to one or more groups of users, wherein the tasks may be assigned to a group of users of said one or more groups of users any one of said one or more users may open the task, wherein the user within said group opens the task before the user can activate a device associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the vulnerability data.

32. The system of claim 29, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user of said one or more users wherein said user can change the way the task list is displayed.

33. The system of claim 29, wherein said one or more users login to the automated workflow system using a login name and a password with said automated workflow system capturing data indicating how long said users remain logged in, where said captured data is used to generate a report.

34. An automated workflow system for monitoring technology information for configuration standards comprising:

an initiator for initiating a configuration standard;

a researcher for researching the configuration standard; and

a documenter for documenting the configuration standard within configuration standard data.

35. The system of claim 34, wherein the automated workflow system further comprises:

a reviewer for reviewing the configuration standard and the configuration standard data;

an editor for editing the configuration standard data;

an approver for approving the configuration standard and the configuration standard data; and

a publisher for publishing the configuration standard and the configuration standard data to a database.

36. The system of claim 34, wherein each device of the workflow system can add reference data including a reference name, reference number and a technology name to the configuration standard data and the device presents reference data to an approver for approval.

37. The system of claim 34, wherein each device of the workflow system can add workflow comments to the configuration standard data and the workflow comments can be displayed by the device of the workflow system with the most recent addition being shown first.

38. The system of claim 34, further comprising technology information added to the configuration standard data in a hierarchical structure, said technology information at least comprising:

vendor information;

product information; and

release information.

39. The system of claim 34, further comprising one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task within said list of tasks is a single configuration standard at a single device within the automated workflow system.

40. The system of claim 39, wherein said one or more users are assigned a level of experience that can be used by the automated workflow system to determine a level of review required for a user.

41. The system of claim 39, wherein said one or more users are assigned to one or more groups of users, wherein the task may be assigned to a group of users any one of whom may open the task, wherein a user within said group opens the task before the user can activate a device associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the configuration standard data.

42. The system of claim 39, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user within said one or more users wherein said user can change the way the task list is displayed.

43. The system of claim 39, wherein said one ore more users login to the automated workflow system using a login name and a password with said automated workflow system capturing data indicating how long each of said users remain logged in,

where said captured data is used to generate a report.

44. A system for developing configuration standards for use with an automated workflow system comprising:

an initiator to initiate a content entry;

a researcher to research the content entry;

a validator to validate the content entry;

an approver to approve the content entry; and

a publisher to publish the content entry to a database of approved configuration standards.

45. A system for updating content within a content management system using an automated workflow system comprising a Content Update System for updating the content within the content management system, wherein said content update system uses a pull methodology allowing systems to obtain updated content when requested rather that pushing data onto said systems.

46. A system for creating policies for use within a content management system using an automated workflow system, comprising:

an initiator for initiating a content entry;

a researcher for researching the content entry;

a validator for validating the content entry;

an approver for approving the content entry; and

a publisher for publishing the content entry to a database of approved policies.

47. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for monitoring technology information for vulnerabilities, the method steps comprising:

detecting a vulnerability;

researching the vulnerability; and

documenting the vulnerability within vulnerability data.

48. The computer system of claim 47, wherein the automated workflow process further comprises:

reviewing the vulnerability and the vulnerability data;

editing the vulnerability data;

approving the vulnerability and the vulnerability data; and

publishing the vulnerability and the vulnerability data to a database.

49. The computer system of claim 47, wherein at each step in the workflow process, reference data including a reference name, reference number and a technology name can be added to the vulnerability data and the reference data will be presented to an approver for approval.

50. The computer system of claim 47, wherein at each step in the workflow process, workflow comments can be added to the vulnerability data and the workflow comments can be displayed during the steps of the workflow process with the most recent addition being shown first.

51. The computer system of claim 47, wherein technology information is added to the vulnerability data in a hierarchical structure, said technology information at least comprising:

vendor information;

product information; and

release information.

52. The computer system of claim 47, wherein automated workflow process steps are performed by one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task is a single vulnerability at a single process step within the automated workflow process.

53. The computer system of claim 52, wherein said one or more users are assigned a level of experience that can be used by the automated workflow process to determine a level of review required for said one or more users.

54. The computer system of claim 52, wherein said one or more users are assigned to one or more groups of users, wherein the tasks may be assigned to a group of users of said one or more groups of users any one of said one or more users may open the task, wherein a user within said group opens the task before the user can perform a process step associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the vulnerability data.

55. The computer system of claim 52, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user of said one or more users wherein said user can change the way the task list is displayed.

56. The computer system of claim 52, wherein said one or more users login to the automated workflow process using a login name and a password with said automated workflow process capturing data indicating how long said users remain logged in, where said captured data is used to generate a report.

57. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for monitoring technology information for configuration standards comprising an automated workflow process for:

initiating a configuration standard;

researching the configuration standard; and

documenting the configuration standard within configuration standard data.

58. The computer system of claim 57, wherein the automated workflow process further comprises:

reviewing the configuration standard and the configuration standard data;

editing the configuration standard data;

approving the configuration standard and the configuration standard data; and

publishing the configuration standard and the configuration standard data to a database.

59. The computer system of claim 57, wherein at each step in the workflow process, reference data including a reference name, reference number and a technology name can be added to the configuration standard data and the reference data will be presented to an approver for approval.

60. The computer system of claim 57, wherein at each step in the workflow process, workflow comments can be added to the configuration standard data and the workflow comments can be displayed during the steps of the workflow process with the most recent addition being shown first.

61. The computer system of claim 57, wherein technology information is added to the configuration standard data in a hierarchical structure, said technology information at least comprising:

vendor information;

product information; and

release information.

62. The computer system of claim 57, wherein automated workflow process steps are performed by one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task is a single configuration standard at a single process step within the automated workflow process.

63. The computer system of claim 62, wherein said one or more users are assigned a level of experience that can be used by the automated workflow process to determine a level of review required for a user.

64. The computer system of claim 62, wherein said one or more users are assigned to one or more groups of users, wherein the task may be assigned to a group of users any one of whom may open the task, wherein a user within said group opens the task before the user can perform a process step associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the configuration standard data.

65. The computer system of claim 62, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user wherein said user can change the way the task list is displayed.

66. The computer system of claim 62, wherein said users login to the automated workflow process using a login name and a password with said automated workflow process capturing data indicating how long said user remains logged in, where said captured data is used to generate a report.

67. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for developing configuration standards for use with an automated workflow process comprising:

initiating a content entry;

researching the content entry;

validating the content entry;

approving the content entry; and

publishing the content entry to a database of approved configuration standards.

68. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for updating content within a content management system using an automated workflow process, wherein content within the content management system is updated by a Content Update System that uses a pull methodology by allowing systems to obtain updated content when requested rather that pushing data onto said systems.

69. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for creating policies for use within a content management system using an automated workflow process, comprising:

initiating a content entry;

researching the content entry;

validating the content entry;

approving the content entry; and

publishing the content entry to a database of approved policies.

69. A computer recording medium including computer executable code for monitoring technology information for at least one of vulnerabilities and configuration standards comprising:

code for performing an automated workflow process for,

at least one of detecting a vulnerability and initiating a configuration standard,

researching at least one of the vulnerability and the configuration standard, and

documenting at least one of the vulnerability within vulnerability data and

the configuration standard within a configuration standard.

70. The computer recording medium of claim 69, wherein the code for performing an automated workflow process further performs:

reviewing the vulnerability and the vulnerability data;

editing the vulnerability data;

approving the vulnerability and the vulnerability data; and

publishing the vulnerability and the vulnerability data to a database.

71. The computer recording medium of claim 69, further comprising code such that at each step in the workflow process, reference data including a reference name, reference number and a technology name can be added to the vulnerability data and the reference data will be presented to an approver for approval.

72. The computer recording medium of claim 69, further comprising code such that at each step in the workflow process, workflow comments can be added to the vulnerability data and the workflow comments can be displayed during the steps of the workflow process with the most recent addition being shown first.

73. The computer recording medium of claim 69, further comprising code for adding technology information to the vulnerability data in a hierarchical structure, the technology information comprising at least one of:

vendor information;

product information; and

release information.

74. The computer recording medium of claim 69, wherein automated workflow process steps are performed by one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task is a single vulnerability at a single process step within the automated workflow process.

75. The computer recording medium of claim 74, wherein said one or more users are assigned a level of experience that can be used by the automated workflow process to determine a level of review required for said one or more users.

76. The computer recording medium of claim 74, wherein said one or more users are assigned to one or more groups of users, wherein the tasks may be assigned to a group of users of said one or more groups of users any one of said one or more users may open the task, wherein a user within said group opens the task before the user can perform a process step associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the vulnerability data.

77. The computer recording medium of claim 74, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user of said one or more users wherein said user can change the way the task list is displayed.

78. The computer recording medium of claim 74, wherein said one or more users login to the automated workflow process using a login name and a password with said automated workflow process capturing data indicating how long said users remain logged in, where said captured data is used to generate a report.

79. The computer recording medium of claim 69, wherein the automated workflow process further comprises code for :

reviewing the configuration standard and the configuration standard data;

editing the configuration standard data;

approving the configuration standard and the configuration standard data; and

publishing the configuration standard and the configuration standard data to a database.

80. The computer recording medium of claim 69, further comprising code such that at each step in the workflow process, reference data including a reference name,

reference number and a technology name can be added to the configuration standard data and the reference data presented to an approver for approval.

81. The computer recording medium of claim 69, further comprising code such that at each step in the workflow process, workflow comments can be added to the configuration standard data and the workflow comments can be displayed during the steps of the workflow process with the most recent addition being shown first.

82. The computer recording medium of claim 69, further comprising code for adding technology information to the configuration standard data in a hierarchical structure, said technology information at least comprising:

vendor information;

product information; and

release information.

83. The computer recording medium of claim 69, wherein automated workflow process steps are performed by one or more users each assigned one or more user roles wherein each one or more users is assigned a list of tasks to perform, wherein, each task within said list of tasks is a single configuration standard at a single process step within the automated workflow process.

84. The computer recording medium of claim 83, wherein said one or more users are assigned a level of experience that can be used by the automated workflow process to determine a level of review required for a user.

85. The computer recording medium of claim 83, wherein said one or more users are assigned to one or more groups of users, wherein the task may be assigned to a group of users any one of whom may open the task, wherein a user within said group opens the task before the user can perform a process step associated with the task and while said task is open, the task is in a locked state and another user within said group cannot open the task and said another user cannot modify the configuration standard data.

86. The computer recording medium of claim 83, wherein said assigned list of tasks to perform comprises a task list that is displayed to a user with said one or more users wherein said user can change the way the task list is displayed.

87. The computer recording medium of claim 83, wherein said one or more users login to the automated workflow process using a login name and a password with said automated workflow process capturing data indicating how long each of said users remain logged in, where said captured data is used to generate a report.

88. A computer recording medium including computer executable code for developing configuration standards in an automated workflow process comprising code for:

initiating a content entry;
researching the content entry;
validating the content entry;
approving the content entry; and
publishing the content entry to a database of approved configuration standards.

89. The method of claim 6, wherein said automated workflow process captures data indicating the length of time for which the automated workflow process steps are performed.

90. The method of claim 16, wherein said automated workflow process captures data indicating the length of time for which the automated workflow process steps are performed.

91. The system of claim 29, wherein said automated workflow process captures data indicating the length of time for which the automated workflow process steps are performed.

92. The system of claim 39, wherein said automated workflow process captures data indicating the length of time for which the automated workflow process steps are performed.

93. The computer system of claim 52, wherein said automated workflow process captures data indicating the length of time for which the automated workflow process steps are performed.

94. The computer system of claim 62, wherein said automated workflow process captures data indicating the length of time for which the automated workflow process steps are performed.